Research on Blockchain Technologies in Bidding Systems

Yi-Hui Chen[1,2], Li-Chin Huang[3], Iuon-Chang Lin[4], and Min-Shiang Hwang[5,6]
(Corresponding author: Min-Shiang Hwang)

Department of Information Management, Chang Gung University, Taoyuan 33302, Taiwan [1]
Kawasaki Disease Center, Kaohsiung Chang Gung Memorial Hospital, Kaohsiung 83301, Taiwan[2]
(Email: cyh@gap.cgu.edu.tw)
Department of Information Management, Executive Yuan, Taipei 10058, Taiwan[3]
Department of Management Information Systems, National Chung Hsing University, Taiwan[4]
Department of Computer Science & Information Engineering, Asia University, Taichung, Taiwan[5]
500, Lioufeng Rd., Wufeng, Taichung 41354, Taichung, Taiwan, R.O.C.
Department of Medical Research, China Medical University Hospital, China Medical University, Taiwan[6]
(Email: mshwang@asia.edu.tw)
(Received Apr. 13, 2020; Revised and Accepted June 21, 2020; First Online June 30, 2020)

Abstract

Due to the popularity of the Internet, people are increasingly accepting the integration of electronic service applications. Whether it is communication, trading, or transportation, these have gradually changed people's lifestyles. Electronic auctions have also become one of the popular e-commerce activities. Electronic auction systems usually include bidders, auctioneers, and third parties that allow bidders to bid via the Internet. It replaces the inconvenience and low efficiency of traditional tendering. Electronic auctions can be divided into two types: open bidding and sealed bidding. The public bidding method is to continuously increase the bidding price until no bidder is willing to pay a higher bid. The deadline has arrived. The highest bidder is the winner of the public tender. Since bidders can bid multiple times, this bidding method is also called multiple bidding. The bidding method for sealed bids is that the bidder can only send the bill once. Once the deadline arrives, the auctioneer will compare all bills. The bidder with the highest bid is the winner of the "sealed bid". Since bidders can only bid once, this bidding method is also called a single bid auction. Both bidding methods have their practicability. But no matter what kind of bidding. It should rely on intermediaries to allow buyers and sellers to conduct transactions. Lead to trust and transaction cost issues. In this regard, we will use blockchain technology to develop smart contracts for public bidding and sealed bidding. It uses the characteristics of blockchain decentralization and low transaction costs to improve the shortcomings of electronic auctions.

Keywords: Bid; Blockchain; E-auction; P2P Network; Public Bid; Sealed Smart Contract

1 Introduction

Due to the popularity of the Internet, most people have gradually accepted electronic integrated applications. Whether it is communication, transaction, or service, it has profoundly changed people's living habits. Electronic bidding has become one of the popular e-commerce activities [1, 8].

Electronic auctions originated from traditional auctions. It is an application that combines Internet technology and auction mechanism to speed up transaction efficiency and speed [2, 3, 14, 18, 23]. It is a trading system that breaks the limitations of time, space, and geography through Internet technology. Therefore, electronic bidding has become an incredibly popular transaction mode in e-commerce.

Electronic bidding is usually composed of bidders, auctioneers, and third parties (see Figure 1). Currently, most e-bidding systems are mainly provided by intermediaries to provide platforms and services. Buyers and sellers can publish, bid, or trade. Popular auction platforms include Yahoo auctions, open-air auctions, and shrimp auctions. However, due to the current need to rely on intermediaries' platforms and services, intermediaries must pay some fees, such as publishing fees, transaction fees, etc. It may cause the problem of increased transaction costs between the buyer and seller [19, 20, 22]. Therefore, this research applies blockchain smart contract technology to electronic bidding [4–7, 15–17, 21, 25]. The use of the blockchain's decentralized nature eliminates the intermediary in electronic bidding, so buyers and sellers can

directly conduct transactions without relying on intermediaries.

Figure 1: The entities in the electronic bidding system

2 Types of Bidding

Electronic bidding can be divided into three main types of bidding:

1) English Auction:
English auctions, also known as price-raising auctions, are the most common and frequently encountered auction method [9,12,24]. During the auction, the price suggested by all bidders must be higher than the previous price. When the auction time expires, the highest bidder will get the item. However, "Sniping" often occurs in online auctions. In other words, until the last few minutes before the auction ends, a specific bidder makes a bid. So there is no time for the remaining bidders to fight back. The solution to this phenomenon is to add an "expansion period" before the original fixed period. For example, if the extension time is set to ten minutes, it means that in the last ten minutes, if there are any bidders, the auction deadline will be automatically extended by ten minutes. This method effectively solves the sniper phenomenon.

2) Dutch Auction:
Dutch auctions are also called reduced price auctions. After a specific time interval, the main feature is that the price will be reduced according to the initially set price reduction rules until the bidder is willing to buy at that price [10,11,13]. This action is more suitable for perishable items such as fruits and vegetables.

   In English auctions, the initial price of the product is usually lower than its market price. After bidders bid with each other, the price will be close to the market price. As prices increase, the number of bidders will also decrease. Dutch auctions are the opposite of English auctions. The initial price of the commodity will be higher than its market price. As the price drops, the number of bidders will increase.

3) Sealed Bid Auction:
In the sealed bid list, the prices of all bidders will be sealed. The prices of all bidders will not be compared before the deadline for the bid opening [8, 14, 18]. Electronically sealed bidding auctions often have a common flaw. Before the bid opening deadline, bidders cannot ensure that their bid prices have been leaked by third parties (leading bidders), which may result in malicious bidders colluding with leading bidders to obtain the best bid price. The research topic aims to use blockchain smart contract technology to ensure the confidentiality, non-repudiation, and non-changeability of electronically sealed bids and solve electronically sealed bids' shortcomings.

With the current development of electronic bidding, two main problems can be found. First of all, the transaction process of electronic bidding must rely on intermediary agencies. It is difficult for buyers and sellers to communicate directly. It also causes problems such as increased transaction costs. Therefore, this research proposes three research topics:

1) Applying blockchain technology to electronic bidding. Using the blockchain's decentralized nature, intermediaries that were originally indispensable for e-bidding have been deleted to reduce transaction costs.

2) In sealed bidding, the bidder cannot ensure that the lousy bidder leaks the bid price. The protection of fair competition may be less. Therefore, this research topic aims to use blockchain smart contracts to improve the shortcomings of sealed bidding. Use the blockchain's immutability to write rules in a sealed bid so that no one can open it before the bid opening time comes to ensure the data's privacy.

3) Use private blockchain to conduct related research on public bidding and sealed bidding.

3 Research on Blockchain Bidding Systems

Due to the rapid development of Internet technology, electronic bidding has replaced traditional bidding. The inconvenient and ineffective bidding mechanism of traditional bidding has been improved. It allows bidders to bid through the Internet anytime and anywhere. Provide bidders and bidders with a faster and more convenient transaction mechanism. However, in the current electronic bidding transaction mechanism, it is necessary to rely on intermediaries to complete the two parties' transactions. Therefore, the following two problems may occur:

1) Trust Issues:
To complete a transaction through an intermediary, you may first need to use personal data to apply for a set of accounts that can be used to use the platform's services. After the transaction is completed, the account's transaction details will be stored in the platform's database. Users may worry that their personal information or transaction records will be leaked out, causing mistrust.

2) Transaction Cost Issue:
In the transaction process, to use the platform's ser-

vices, users may need to pay some platform publishing fees, advertising fees, or transaction fees. It may lead to higher transaction costs between buyers and sellers.

In response to the above two electronic bidding issues, this research aims to use the characteristics of blockchain decentralization and zero trust foundation to develop an electronic bidding system based on blockchain smart contract applications to solve the trust problem and reduce transaction costs. The following subsections will illustrate the implementation methods and steps of these research topics.

3.1 Research on Smart Contracts for Public Bidding

A complete public bidding e-bidding mechanism has the following basic requirements:

1) The identity of the bidder during the bidding process is anonymous. After the bidding is over, the bidders and successful bidders are anonymous.
2) During the sending process, the content of the bid list cannot be changed. Everyone can verify the source of the bid and the correctness and completeness of the content.
3) No one can pretend to be a legitimate bidder. After bidding, the bidder cannot deny that the bid has been submitted.
4) The bidder must prove that he has submitted his bid or prove that he has won the bid.
5) After winning the bid, the bidder can ask for money from the winning bidder, but the bidder cannot ask for money from the winning bidder.

The electronic bidding process of public bidding is shown in Figure 2. In the beginning, the bidding meeting announced bidding information, including product descriptions and starting prices. After that, the bidder can continue to bid. The bidder will receive the bid submitted by the bidder. And send a message to the bidder notifying that the bid has been received. And announce the current highest bid to everyone. Before any bidder offers a higher price, the bidder will announce the final bid price. And collect money from the winning bidder, and send the goods to the winning bidder after confirmation.

The first research topic is the study of smart contracts for public bidding on the blockchain. This research will develop public bidding through blockchain smart contract development. Write the public bidding transaction contract on the blockchain. Use peer-to-peer technology to achieve the purpose of decentralization. All bidders can bid by calling this public bidding transaction contract without relying on intermediary agencies. To this end, the steps of this study are as follows:

1) Create an Account:
   The process of creating an account. Use the Ethereum wallet to create two blockchain accounts to facilitate subsequent testing, transactions, etc.
2) Mining:
   Use the command line and MinerGate to perform mining. Get currency to pay commissions when creating contracts and transactions.
3) Perform Block Synchronization and View Block Status:
   At this stage, use the command line to synchronize the blocks. After that, you can enter a block to view the detailed information in that block.
4) Create a Smart Contract:
   Establishing a smart contract is mainly divided into three execution steps: writing, compiling and deploying. Use Sublime to write the Solidity programming language. Then use the Solidity real-time compiler and runtime to compile the agreement into Bytecode and Interface. Finally, use the Ethereum wallet to deploy the contract and publish the contract to the blockchain.
5) Test Contract:
   When the contract is verified in the contract testing phase, the contract's address can be obtained. Use the previously created Account 2 wallet and the interface obtained by compiling Solidity to add the contract to test its related functions.
6) The Structure of Smart Contracts for Public Bidding:
   Figure 3 shows the program structure of the open bid smart contract in our system. The contract is mainly divided into initialization and contract functions.

In the initialization data, the following data will be announced in advance:

- Auctioneer: It is used to record the address of the bidder who initiated the contract.
- AuctionStart: It is used to announce the start time of the bidding.
- bidding time: It is used to announce the significant time of the contract.
- maximumBidder: It is used to record the address of the current highest bidder.
- maximumBid: It is used to record the current maximum price.

In the contract function, the following information will be announced in advance:

- Bid(): Anyone can call this function to perform bidding operations. Before executing this function, first, use AuctionStart and bid time to determine whether the contract expires. If not, the bidder can enter the

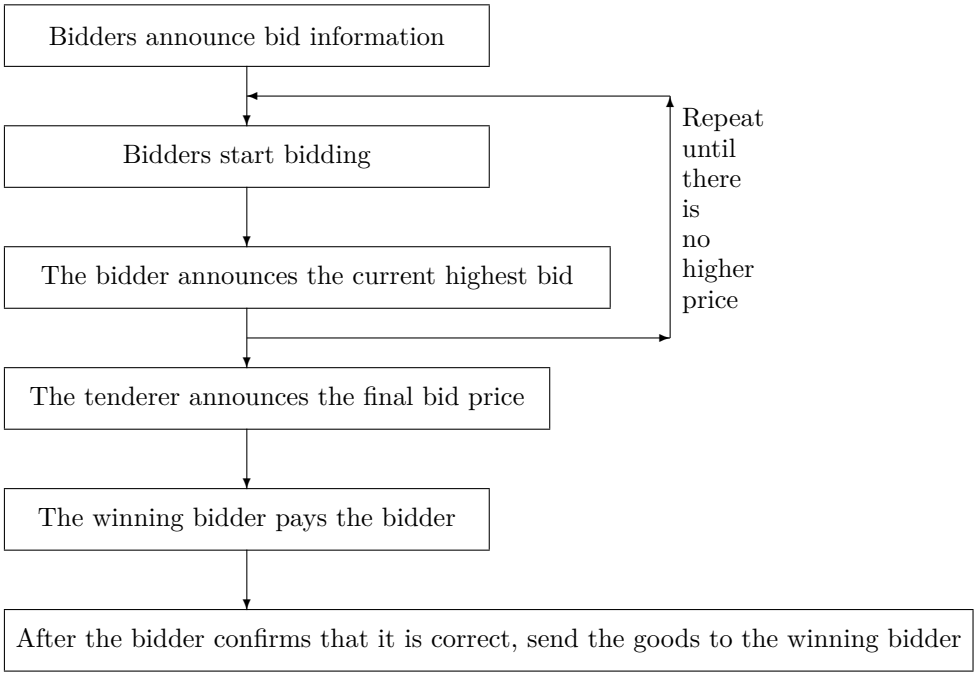

Figure 2: Public bidding process

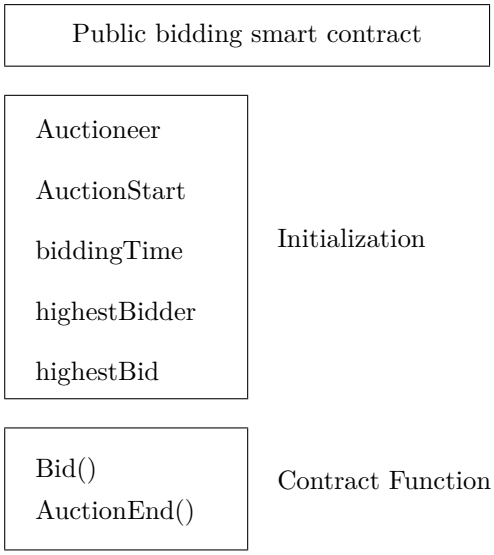

Figure 3: Contract structure of public bidding

bid amount. If the price is greater than the current highest price, the highest bid and highest bidder will be used to record the bidder's amount and address.

- AuctionEnd(): In this function, AuctionStart and bid time are automatically used to determine the contract's sufficient time. If the significant time is over, the winning bidder's address and the amount will be automatically sent to the bidder. This function will be turned off to avoid repeated execution.

It is expected that potential problems will be encountered when conducting this research. The following is an explanation of the solutions to these problems: In a public tender, each bidder can make multiple bids. Therefore, during contract testing, multiple accounts need to be used for mutual bidding. On the public chain, a small fee is required for each execution of an instruction. Therefore, mining operations must be performed on each account. In this way, too much time is spent testing the contract. To this end, this research will first use a testnet to test the contract. Save mining time for each account. After the test is completed, deploy the completed smart contract on the leading blockchain network.

3.2 Research on Smart Contracts with Sealed Bids

A complete sealed bidding mechanism has the following basic requirements:

1) Throughout the bidding process, the identities of bidders and successful bidders are anonymous.

2) During the transfer process, the content of the bid list cannot be changed. Everyone can verify the source of the bid and the correctness and completeness of the content.

3) No one can pretend to be a legitimate bidder. After bidding, the bidder cannot deny that the bid has been submitted.

4) The bidder must prove that he has submitted his bid or prove that he has won the bid.

5) Bids must be delivered within a significant time; expired bids are invalid.

6) Before the bid is opened, no one can open the bid.

7) When encountering the same price, there must be a fair solution.

The bidding process for sealed bidding is shown in Figure 4. In the beginning, the bidders announced the bid information, including product descriptions and starting prices. Bidders who want to participate in the bidding must first register with the exhibition agency. After the identity is confirmed, all legal bidders can bid before the deadline for bidding. All bids will be encrypted and then sent to bidders. All encrypted bids will be unlocked before the bid opening, and the final winner can be determined after comparison.

In the sealed bidding mechanism, it is necessary to rely on impartial intermediary agencies to assist. However, it is also possible that the tender and the impartial agency may conspire to disclose bid information in the bid before the bid opening. Therefore, the second research topic is the study of smart contracts with sealed bidding on the blockchain. Sealed bidding will be developed through blockchain smart contracts. Use the decentralized function of the blockchain to improve this problem. The steps of this research are as follows:

1) Extend the first research topic into mining, contract writing, contract preparation, and contract deployment.

2) Seal the structure of the smart bidding contract. Figure 5 shows the program structure of the sealed bid smart contract in the research system. The contract is mainly divided into initialization and contract functions.

In the initialization data, we declare the following data in advance:

- auctioneer:It is used to record the address of the bidder who initiated the contract.
- auctionStart: It is used to announce the start time of the auction.
- biddingTime: It is used to announce the contract time.
- bididngEnd: It is used to announce the bidding time of the contract.
- maximumBidder: It is used to record the address of the current highest bidder.
- maximumBid: It is used to record the current maximum price.

In the contract function, the following information will be announced in advance:

- blindAuction(): Activate the contract by calling this function. And use auctionStart and biddingEnd to record the start and end time.
- bid(): The bidder can call this function to perform bidding operations.
- Reveal (): Perform bid opening action by calling this function. And compare the prices of all bids to get the final bidder.
- auctionEnd(): By calling this function, the number and addresses of successful bidders will be collected.
- withdraw(): Refund the bid amount of someone other than the winning bidder.

It is expected that potential problems will be encountered in the implementation of this research. The following is an explanation of these problems: In a sealed bid smart contract, the contract's function is more complicated. For bidders and bidders, the wrong contract function may be called. For example, the bidder accidentally called show() to open all bids, so bids must be terminated and redeployed. To this end, this research will establish authority judgments for different functions. Before executing this function, it will determine whether the caller can execute this function.

3.3 Research on Public Bidding and Private Chain Public Bidding

The public chain is an open node. Anyone can enter other nodes to view transaction status and contract content. Therefore, the privacy of smart contract code may not be protected and may be abused by others. Therefore, the study of public bidding and sealed bidding on the private chain will use the private chain to develop smart contracts for public bidding and sealed bidding. Use the command line to create a dedicated chain. Use the characteristics of a dedicated chain to control the write and read permissions of the node. They are used to protect private transaction records and smart contract content.

It is expected that this study will encounter some potential problems. The following is an explanation of the solutions to these problems: At present, most blockchain

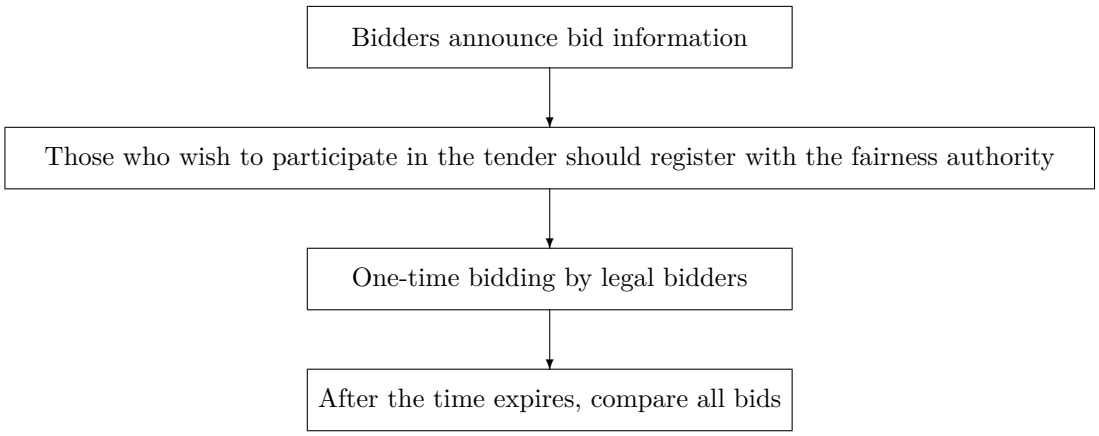

Figure 4: The bidding process for a sealed bid

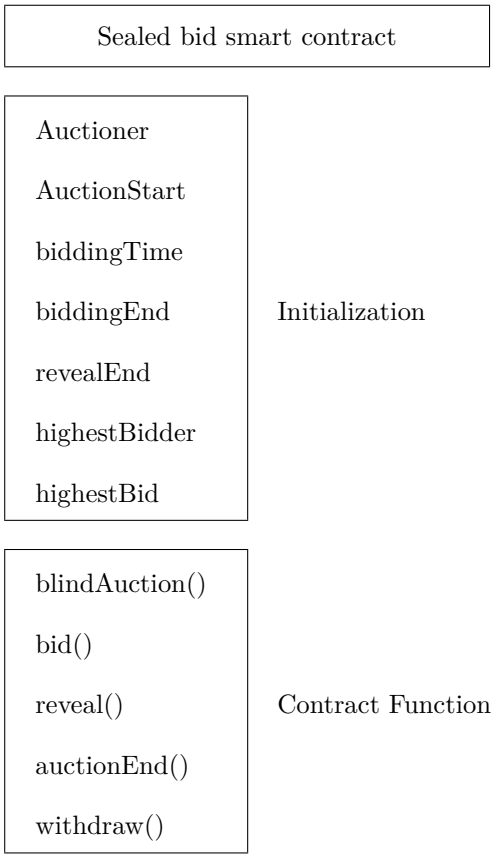

Figure 5: Contract structure of a sealed bid

smart contracts focus on the research of public chains, and there is less literature on private chain smart contracts. Therefore, there is less content to be cited. It requires repeated research to find the best solution. This research aims at the application of Ethereum token in private chain contract testing.

4 Conclusions

In this article, we have proposed three research topics: 1) Research on smart contracts for public bidding; 2) Research on smart contracts with sealed bids; 3) Research on public bidding and private chain public bidding.

This research deployed smart contracts on public and private chains. Use the respective characteristics and advantages of public and private chains to develop applications suitable for different fields. This research uses blockchain smart contracts to improve the shortcomings of the e-bidding system. Replace the transaction mechanism that previously relied on a third party. It not only solves the issue of trust enforcement between the parties to the transaction. It can also reduce transaction costs. The results of this research can be applied in many fields. For example, it can be applied to cross-border remittances, contract insurance policies, and loan credit in the financial market. The industrial supply chain can be applied to product history tracking and supply a collaborative chain supply.

Acknowledgments

The Ministry of Science and Technology partially supported this research, Taiwan (ROC), under contract no.: MOST 108-2410-H-468-023 and MOST 108-2622-8-468-001-TM1.

References

[1] G. Cao and J. Chen, "Practical electronic auction scheme based on untrusted third-party," in *International Conference on Computational and Information Sciences*, pp. 493-496, 2013.

[2] T. S. Chandrashekar, Y. Narahari, C. H. Rosa, D. M. Kulkarni, J. D. Tew and P. Dayama, "Auction-based mechanisms for electronic procurement," *IEEE Transactions on Automation Science and Engineering*, vol. 4, no. 3, pp. 297-321, 2007.

[3] W. Chen and F. Lei, "A simple efficient electronic auction scheme," in *Eighth International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT'07)*, pp. 173-174, 2007.

[4] Y. H. Chen, L. C. Huang, I. C. Lin, and M. S. Hwang, "Research on the secure financial surveillance blockchain systems," *International Journal of Network Security*, vol. 22, no. 4, pp. 708-716, 2020.

[5] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292-2303, 2016.

[6] P. Fan, Y. Liu, J. Zhu, X. Fan, and L. Wen, "Identity management security authentication based on blockchain technologies," *International Journal of Network Security*, vol. 21, no. 6, pp. 912-917, 2019.

[7] C. Hu, D. Zheng, R. Guo, A. Wu, L. Wang, and S. Y. Gao, "A novel blockchain-based anonymous handover authentication scheme in mobile networks," *International Journal of Network Security*, vol. 22, no. 5, pp. 874-884, 2020.

[8] X. Hu, Z. Qin, F. Zhang, Y. Yang, and Y. Zhao, "A sealed-bid electronic auction protocol based on ring signature," in *International Conference on Communications, Circuits and Systems*, pp. 480-483, 2007.

[9] M. S. Hwang, E. J. L. Lu, I. C. Lin, "Adding timestamps to the secure electronic auction protocol", *Data & Knowledge Engineering*, vol. 40, no. 2, pp. 155-162, Feb. 2002.

[10] W. Jiang, J. Chen, Y. Xu, Y. Wang, L. Tan, "Research on the influence factors of consumer repurchase in Dutch auction", *Lecture Notes in Computer Science*, vol. 11354, pp. 330-338, 2019.

[11] C. C. Lee, P. F. Ho, M. S. Hwang, "A secure E-auction scheme based on group signatures," *Information Systems Frontiers*, vol. 11, no. 3, pp. 335-343, July 2009

[12] C. C. Lee, M. S. Hwang, C. W. Lin, "A new English auction scheme using the bulletin board system", *Information Management and Computer Security*, vol. 17, no. 5, pp. 408-417, Nov. 2009.

[13] C. C. Lee, M. S. Hwang, C. W. Lin, "An efficient multi-round anonymous auction protocol", *Journal of Discrete Mathematical Sciences & Cryptography*, vol. 10, no. 4, pp. 547-557, Aug. 2007.

[14] S. Li, X. Li, M. X. He, S. K. Zeng and X. L. Tang, "Sealed-BID electronic auction without the third party," in *11th International Computer Conference on Wavelet Actiev Media Technology and Information Processing (ICCWAMTIP'14)*, pp. 336-339, 2014.

[15] Z. C. Li, J. H. Huang, D. Q. Gao, Y. H. Jiang and F. Li, "ISCP: An improved blockchain consensus protocol," *International Journal of Network Security*, vol. 21, no. 3, pp. 359-367, 2019.

[16] I. C. Lin and T. C. Liao, "A survey of blockchain security issues and challenges," *International Journal of Network Security*, vol. 19, no. 5, pp. 653-659, 2017.

[17] Y. Liu, M. He, and F. Pu, "Anonymous transaction of digital currency based on blockchain," *International Journal of Network Security*, vol. 22, no. 3, pp. 444-450, 2020.

[18] W. Shi, I. Jang and H. S. Yoo, "A sealed-bid electronic marketplace bidding auction protocol by using ring signature," in *Fourth International Conference on Computer Sciences and Convergence Information Technology*, pp. 1005-1009, 2009.

[19] W. K. Tan and Y. L. Chung, "User payment choice behavior in e-auction transactions," in *International Conference on e-Education, e-Business, e-Management and e-Learning*, pp. 183-187, 2010.

[20] C. C. Tu, C. Y. Lin and K. Fang, "Customers' perception on attitude towards e-auction," in *IEEE Asia-Pacific Services Computing Conference*, pp. 1044-1048, 2008.

[21] L. Wang, D. Zheng, R. Guo, C. Hu, and C. M. Jing, "A blockchain-based privacy-preserving authentication scheme with anonymous identity in vehicular networks," *International Journal of Network Security*, vol. 22, no. 6, pp. 981-990, 2020.

[22] S. Yao, W. A. Cui and Z. Wang, "A model in support of bid evaluation in multi-attribute e-auction for procurement," in *4th International Conference on Wireless Communications, Networking and Mobile Computing*, pp. 1-4, 2008.

[23] F. Zhang, Q. Li and Y. Wang, "A new secure electronic auction scheme," in *IEEE/AFCEA Information Systems for Enhanced Public Safety and Security (EUROCOMM'00)*, pp. 54-56, 2000.

[24] H. Zhong, S. Li, T. F. Cheng, C. C. Chang, "An efficient electronic English auction system with a secure on-shelf mechanism and privacy preserving", *Journal of Electrical and Computer Engineering*, vol. 2016, 2016.

[25] Y. Zhu, R. Guo, G. Gan and W. T. Tsai, "Interactive incontestable signature for transactions confirmation in bitcoin blockchain," in *IEEE 40th Annual Computer Software and Applications Conference (COMPSAC'16)*, pp. 443-448, 2016.

Biography

Yi-Hui Chen received her Ph.D. degree in computer science and information engineering at the National Chung Cheng University. Later on, she worked at Academia

Sinica as a post-doctoral fellow. Then, she worked at IBM's Taiwan Collaboratory Research Center as a Research Scientist, the Department of M-Commerce and Multimedia Applications, Asia University as an associate professor. She is now an associate professor at the Department of Information Management, Chang Gung University. Her research interests include multimedia security, semantic web, text mining, and multimedia security.

Li-Chin Huang received the B.S. in computer science from Providence University, Taiwan, in 1993 and M.S. in information management from Chaoyang University of Technology (CYUT), Taichung, Taiwan, in 2001; and the Ph.D. degree in computer and information science from National Chung Hsing University (NCHU), Taiwan in 2001. Her current research interests include information security, cryptography, medical image, data hiding, network, security, big data, and mobile communications.

Iuon-Chang Lin received the B.S. in Computer and Information Sciences from Tung Hai University, Taichung, Taiwan, Republic of China, in 1998; the M.S. in Information Management from Chaoyang University of Technology, Taiwan, in 2000. He received his Ph.D. in Computer Science and Information Engineering in March 2004 from National Chung Cheng University, Chiayi, Taiwan. He is currently a professor of the Department of Management Information Systems, National Chung Hsing University, and Department of Photonics and Communication Engineering, Asia University, Taichung, Taiwan, ROC. His current research interests include electronic commerce, information security, cryptography, and mobile communications.

Min-Shiang Hwang received M.S. in industrial engineering from National Tsing Hua University, Taiwan in 1988, and a Ph.D. degree in computer and information science from National Chiao Tung University, Taiwan, in 1995. He was a professor and Chairman of the Department of Management Information Systems, NCHU, during 2003-2009. He was also a visiting professor at the University of California (UC), Riverside, and UC. Davis (USA) during 2009-2010. He was a distinguished professor of the Department of Management Information Systems, NCHU, during 2007-2011. He obtained the 1997, 1998, 1999, 2000, and 2001 Excellent Research Award of National Science Council (Taiwan). Dr. Hwang was a dean of the College of Computer Science, Asia University (AU), Taichung, Taiwan. He is currently a chair professor with the Department of Computer Science and Information Engineering, AU. His current research interests include information security, electronic commerce, database and data security, cryptography, image compression, and mobile computing. Dr. Hwang has published over 300+ articles on the above research fields in international journals.